INFORMATION SYSTEM SECURITY & ASSURANCE

Gregg Gunsch
Assistant Professor
PhD, University of Illinois at Urbana-Champaign, 1991

- Information Survivability
- Information Warfare
- Computer Forensics
- Artificial Intelligence
- Machine Learning

e-mail: Gregg.Gunsch@afit.edu
phone: 937-255-6565 x 4281

Information Warfare

". . . attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."

“True excellence is to plan secretly, to move surreptitiously, to foil the enemy’s intentions and balk his schemes, so that at last the day may be won without shedding a drop of blood.”

Sun Tzu, The Art of War

The Department of Defense is quickly moving towards a robust global interconnectivity, fueled by ubiquitous computing and communications systems, that promises to provide the capability to collect, process, and disseminate an enormous, uninterrupted flow of information. This empowers a remarkable strategic and tactical C2 advantage, but also becomes a target for disruption and exploitation. The information, information systems, and information processes must be protected to ensure their availability, integrity, authentication, confidentiality, and nonrepudiation.

One area currently being researched addresses computer network intrusion/misuse detection. Network intrusion detection systems (IDSs) monitor data traffic to identify suspicious behavior related to an intrusion attempt, network attack, or pre-assault reconnaissance. Conventional IDSs are overwhelmed by the sheer volume of data and do not scale well for large, distributed networks. Of particular concern in those networks is the distributed, coordinated activity occurring over a protracted time and from many different sources. The use of distributed agents and machine learning holds promise for detecting and responding to these "low and slow" attacks.

Another concern being researched is the ability of the human operator to continue to work effectively in the presence or suspicion of tainted information. Humans tend to trust the information presented to them via computer, and are generally ineffective at recognizing bad information. When it does become apparent, trust in the system is lost and productivity can plummet. We are constructing models of human trust with the intention of developing methods of inducing appropriate levels of skepticism. In addition, artificial intelligence techniques may make it feasible for the computer to detect tainted information and assist the user in maneuvering around the suspect data to produce good decisions despite the corruption.

Facilities

The primary venue for both research and hands-on classroom applications is the LISSARD: Laboratory for Information System Security/Assurance Research and Development. It contains an isolated network in an East Coast-West Coast configuration, supporting over ten high-end PCs and SparcStations, with a variety of operating systems found in the USAF inventory. The LISSARD provides a safe environment to experiment with computer security related tools and techniques, including those for penetration testing, vulnerability analysis, intrusion detection and computer forensics, as well as suites of hacking tools and live viruses.

Henry Potoczny
Professor
PhD, University of Kentucky, 1969

- Computer and data security
- Cryptography
- Steganography

e-mail: Henry.Potoczny@afit.edu
phone: 937-255-6565 x 4282

Additional departmental researchers include:

- **Profs Richard Raines and Rusty Baldwin** (computer network performance and vulnerability analysis)

Interdepartmental

- **Prof David Biros** (information resource management, user trust and skepticism)
- **Prof Richard Deckro** (information operations, operational sciences)